

Informe

¿DÓNDE ESTÁN MIS DATOS?

2021: una mirada retrospectiva a la pandemia

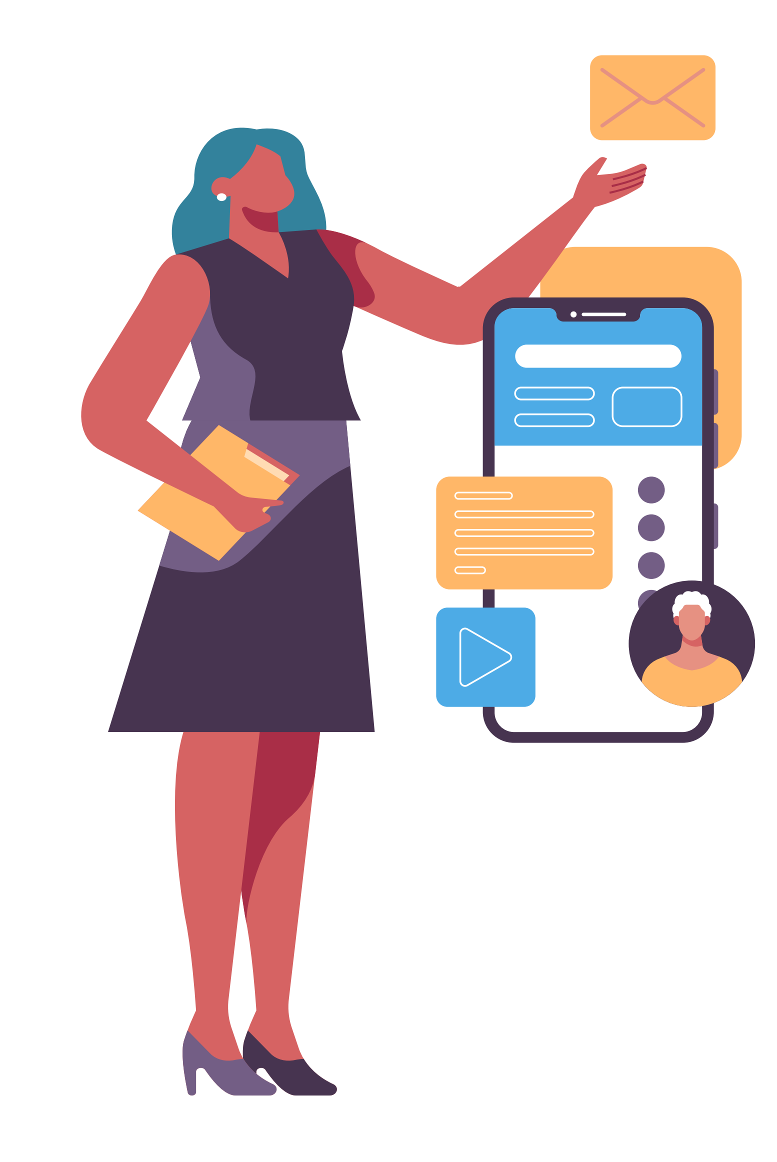
Autoras: Carolina Botero Cabrera y Lucía Camacho Gutiérrez
Investigación: Camila Pérez Failach

Informe

¿DÓNDE ESTÁN MIS DATOS?

2021: una mirada retrospectiva a la pandemia

Un informe de Fundación Karisma que evalúa el compromiso de las empresas proveedoras del servicio de internet con los derechos a la libertad de expresión, intimidad y seguridad digital de sus suscriptores.



Un informe de:

Fundación Karisma

Con el apoyo de:



Fundación Karisma hace un reconocimiento especial a otros proyectos similares que han servido como inspiración: **¿Quién defiende tus datos?** de R3D México, **¿Quién defiende tus datos?** de TEDIC Paraguay, **Quem defende seus dados?** de Internet LAB Brasil, **¿Quién defiende tus datos?** de Hiperderecho Perú, **¿Quién defiende tus datos?** de Derechos Digitales Chile, **¿Quién defiende tus datos?** de ADC Digital Argentina, **¿Quién defiende tus datos?** Panamá y, a otros fuera de la región como **¿Quién defiende tus datos?** de Eticas Foundation España, **Who has your back?** de la Electronic Frontier Foundation y **Ranking Digital Rights** del Open Technology Institute.

También agradece a las personas de las empresas evaluadas que se reunieron con el equipo de trabajo de la Fundación y que han estado trabajando en mejorar los resultados de este ejercicio.

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema: http://www.documentoaccesible.com/#que-es.



Autoras:

Carolina Botero Cabrera

Lucía Camacho Gutiérrez

Investigación:

Camila Pérez Failach

Revisión:

Veridiana Alimonti

Catalina Moreno

Juan DeBrigard

Coordinación Editorial:

Alejandra Martínez Hoyos

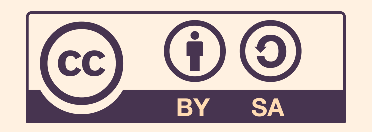
Diagramación y diseño gráfico:

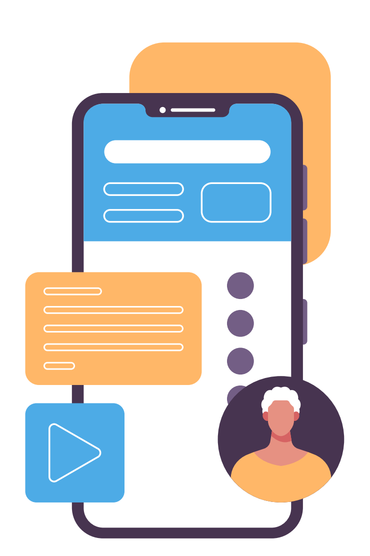
Hugo A. Vásquez Echavarría

Bogotá, Colombia

Marzo de 2022

Con el apoyo especial de Electronic Frontier Foundation





Contenido

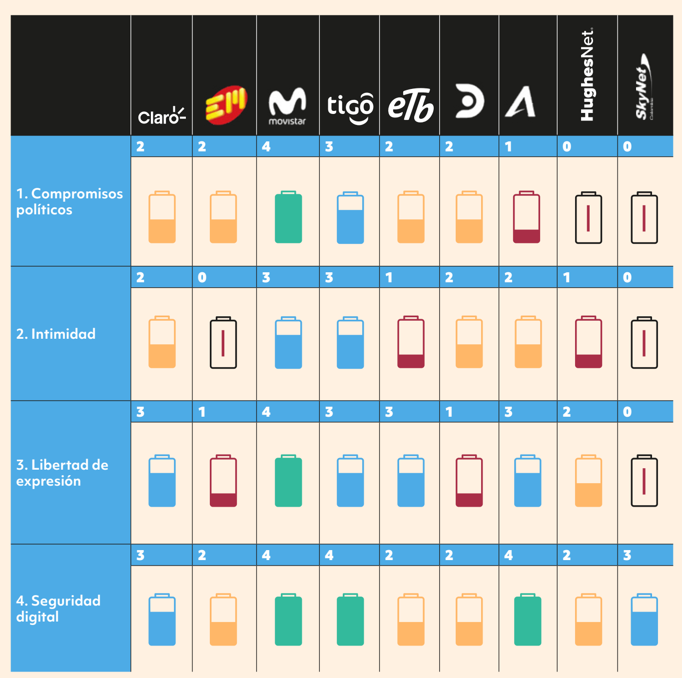
Resumen ejecutivo

El primer año de pandemia supuso para la elaboración de esta nueva edición de "*¿Dónde están mis datos?*" múltiples retos. El más relevante, quizá, tiene que ver con la integración de nuevos ejes de evaluación para documentar la forma en que las medidas desplegadas por el gobierno nacional para la contención de la pandemia impactaron en los compromisos de los proveedoras de servicios de internet (PSI) en materia de transparencia, libertad de expresión, intimidad y seguridad digital.

En nuestro balance general de la información que las empresas publicaron en 2021 sobre lo sucedido en el año 2020, primer año de la pandemia, vimos que en relación con criterios de evaluación tradicionales no se presentaron muchos cambios. Varias empresas mantuvieron su desempeño, incluso aquellas que todavía se encuentran en rezago ante la publicación, por ejemplo, de su informe anual de transparencia, o de políticas de protección de datos con mínimos que están previstos en la ley. Las novedades más relevantes fueron documentadas en torno precisamente de los nuevos ejes de evaluación: neutralidad de la Red y acceso directo.

Los resultados del informe

En 2021 la empresa que mejor puntaje obtuvo, en general, fue Movistar, seguida por Claro y Tigo que comparten un puntaje similar.



	Claro	EM	movistar	tigo	eTb			HughesNet	SkyNet
1. Compromisos políticos	2	2	4	3	2	2	1	0	0
2. Intimidad	2	0	3	3	1	2	2	1	0
3. Libertad de expresión	3	1	4	3	3	1	3	2	0
4. Seguridad digital	3	2	4	4	2	2	4	2	3

1.1. Compromisos políticos

En materia de género y accesibilidad destacan particularmente Movistar y Tigo, seguidos de Claro, ETB y DirecTV que comparten un mismo lugar.

En relación con los informes de transparencia Movistar sigue siendo la empresa con el mejor puntaje. Informa de manera plena sobre todos los criterios esperados y de forma desagregada, incluyendo los eventos de bloqueo ante la declaración de estados de emergencia o excepción. Claro y Tigo compiten con un mismo puntaje en este eje.

En relación con la neutralidad de la Red, que es un nuevo eje de evaluación, destacamos particularmente los casos de Movistar, Tigo, Avantel y Hughesnet que además de publicar sus prácticas de gestión del tráfico hacen expreso su compromiso por proteger dicho principio.

1.2. Intimidad

En el primer eje de evaluación sobre protección de datos debemos indicar que en comparación con los hallazgos del año anterior no se produjeron cambios, por tanto Claro, Movistar, Tigo, ETB, Emcali, Avantel y DirecTV recibieron el mismo puntaje dada la ausencia de modificaciones en sus políticas de tratamiento de datos.

Sobre la evaluación en materia de retención de datos tanto Claro, Movistar como Tigo informan que están obligadas por ley a retener datos en indicación del marco legal, mientras que ETB menciona en su política de tratamiento de datos que retiene datos sin indicación del marco legal.

En relación con el nuevo eje de evaluación en el que buscamos que se informe a las personas usuarias de los servicios de estas empresas sobre la existencia del acceso directo que efectúa la Fiscalía General de la Nación para interceptar comunicaciones, resaltamos que en este criterio de evaluación destaca el caso de Movistar, por la claridad en la información que entrega de este tema y reconocemos que tanto Claro como Tigo también dan información sobre diferencias en el marco jurídico que habilita a esta modalidad de vigilancia de comunicaciones. El caso de Tigo es especial, pues se encuentra además reforzado por el informe mundial de su empresa matriz, Millicom.

En relación con las solicitudes de datos por parte de entidades públicas, procedimiento de entrega y notificación a las personas sobre dichos eventos, durante 2021 los PSI no efectuaron cambios significativos en sus políticas sobre entrega de datos en comparación con la información que ya ofrecían.

1.3. Libertad de expresión

En este eje se analiza la obligación legal de bloqueo y el procedimiento de bloqueo que siguen los PSI. En nuestra revisión encontramos que Claro, Movistar, Tigo, ETB y Avantel informan sobre la ejecución de órdenes de bloqueo de sitios web o URL. Emcali y Hughesnet informan que bloquean sitios web o URL solo en el caso de circulación de contenido de abuso sexual infantil. Skynet no provee información sobre ninguno de estos criterios.

1.4. Seguridad digital

Encontramos que todos los PSI evaluados han implementado el protocolo *https* en sus sitios web.

De otra parte en relación con la evaluación sobre si las compañías informan las fugas de datos personales y acciones de mitigación en caso de que se presenten, si tienen protocolos de notificación a las autoridades cuando suceden fallas de seguridad que comprometen los datos personales de las perso-

nas usuarias de los servicios, así como si las notifican sobre estos sucesos luego de que hayan desplegado las debidas medidas de mitigación, encontramos que Movistar, Tigo y Avantel son las únicas que cuentan con un protocolo y documentación para realizar acciones de mitigación y bloqueos. Skynet advierte en general qué medidas de seguridad despliega pero no cuáles son las de contingencia que aplicaría para posibles brechas de seguridad.

2. Los nuevos criterios de evaluación del informe

La evaluación sobre la *neutralidad de la Red* apuntó a verificar si los PSI publicaron durante 2021 sus prácticas de gestión del tráfico y si asumieron un compromiso más activo por la garantía de uno de los principios fundantes de la Red que aseguran que el tráfico de contenidos, servicios y aplicaciones no sea discriminado de manera arbitraria. Se trata de un principio que se vio amenazado por la regulación de emergencia que previó su suspensión temporal producto, en esencia, de los temores de las autoridades que dudaron de la capacidad de la red para soportar un tráfico de mucho más elevado y constante de personas.

De otra parte, la evaluación sobre el *acceso directo* es nuestro primer acercamiento de documentación sobre una práctica de vigilancia de comunicaciones muy controversial y de dudosa constitucionalidad. Analizamos la información de los últimos informes *¿Dónde están mis datos?* para concluir que en Colombia las autoridades interceptan las comunicaciones de las personas usuarias de los servicios de telecomunicación vía celular, sin mediar orden alguna. Se trata de un tipo de vigilancia masiva de las comunicaciones que ha sido ampliamente cuestionada a nivel internacional, tanto por los organismos internacionales de derechos humanos como por empresas del sector.

3. Otros puntos a resaltar del informe

En esta nueva edición creemos que los operadores que han consolidado buenas prácticas, compatibles con la ley, deben poder apuntar sus acciones de mejora a la granularidad y detalle con que informan sobre cada situación que evaluamos, por ejemplo, desagregando las órdenes de bloqueo a sitios web y URL según qué autoridad la emite. O a través de información mucho más precisa sobre los terceros con los que comparten los datos de las personas que suscriben sus servicios, más allá de las fórmulas genéricas. Las empresas que, por su parte, no han avanzado en compromisos de base tienen cada año un reto más grande, que es el de cerrar la brecha que las separa de aquellas otras con buen desempeño. Algo que sabemos, no se logra de golpe.

Nuestras recomendaciones finales apuntaron a un mismo objetivo: se precisa aumentar los esfuerzos en favor de la transparencia, pues ésta es un instrumento clave para el ejercicio y la defensa de otros derechos.

Las personas que suscriben los servicios de telecomunicaciones precisan saber, por ejemplo, cuándo y en qué ocasiones las autoridades públicas han requerido acceso a sus datos personales, especialmente con motivo de la pandemia, y en qué ocasiones los PSI han rechazado la entrega por su incompatibilidad con los derechos de privacidad y protección de datos de éstos. O necesitan mayor información sobre cuántas órdenes de bloqueo de sitios web han sido emitidas por las autoridades y cuántas de ellas han sido inaplicadas por los PSI por su incompatibilidad en el ejercicio de derechos como el de la libertad de expresión, por citar un caso.

Nuestro informe además sembró el terreno para futuros criterios de evaluación de próximas ediciones. Por último, queremos agradecer a las compañías que en esta edición decidieron seguir de cerca nuestras recomendaciones a través de “pequeños grandes cambios” que redundarán, en adelante, en la protección de los derechos de quienes suscriben sus servicios.

Sobre el informe

¿Dónde están mis datos en la pandemia?

La declaración de la pandemia a inicios de 2020 condujo a la imposición de limitaciones extraordinarias al ejercicio de derechos. Desde las restricciones al libre tránsito hasta la suspensión de toda actividad que implicase el contacto humano fuera de casa: educación, trabajo, justicia, entretenimiento, etc.

La gran mayoría de actividades se vieron forzadas a la virtualidad, y si bien es cierto que dicho traslado enfrentó -según cada actividad- más o menos retos, todas tuvieron en común el uso de una misma herramienta que, al tiempo, es un espacio de encuentro: Internet.

La pandemia significó una presión sobre la Internet que se reflejó en al menos dos formas: el aumento de la demanda de acceso al servicio, y el mayor apetito de los Estados por acceder a los datos de las telecomunicaciones.

En relación con la primera forma de presión, creamos un nuevo criterio de evaluación en nuestro informe para incorporar el compromiso con la neutralidad de la red y que describiremos más adelante.

La segunda forma de presión fue producto de cómo las solicitudes de datos en manos de los proveedores al servicio de internet integró rápidamente la caja de herramientas del Estado para hacer frente a la pandemia.

En este sentido, a finales de marzo de 2020 se emitió la Circular Externa 001 por la Superintendencia de Industria y Comercio (SIC) que ordenaba a responsables del tratamiento de datos personales tanto en el sector público como privado el "suministro de información al Departamento Nacional de Planeación (DNP) y demás entidades estatales que las requieran para atender, prevenir, tratar o controlar la propagación del COVID-19 (coronavirus) y mitigar sus efectos". Lo que interpeló, por supuesto, a las empresas de telecomunicaciones.

Por los medios de comunicación supimos que algunas autoridades locales[1] apuntaban a obtener los datos de las personas que fueran beneficiarias de ayudas sociales con motivo de la pandemia, un fin loable que, sin embargo, era ampliamente superado con el alcance de la autorización dada por la SIC. Esta situación nos llevó a varias organizaciones de la sociedad civil a calificar este acto de "cheque en blanco" que no cumplía con los estándares de una respuesta proporcional, necesaria y no discriminatoria del gobierno durante la emergencia sanitaria[2].

La Circular finalmente no fue aplicada respecto de los PSI pues, frente a la presión de la sociedad civil

1 Ver, por ejemplo, el caso de la Alcaldía de Bogotá en donde se mencionó la necesidad de que los PSI entregaran las bases de datos de todos sus abonados celulares para notificar a las personas sobre la entrega de subsidios económicos en atención a la contingencia económica que significó para muchas personas el cese de sus actividades. Ver video aquí.

2 Se puede consultar este análisis en https://web.karisma.org.co/organizaciones-de-la-sociedad-civil-rechazan-circular-de-la-sic-sobre-uso-de-datos-personales-para-controlar-la-pandemia/

parece que se desplegaron alternativas menos invasivas de la privacidad de las personas suscriptoras de las compañías de telecomunicaciones, y que trasladó a éstas la tarea de envío de las notificaciones sobre la disponibilidad de subsidios económicos tan solo respecto de ciertos abonados celulares, sin mediar la entrega de sus bases de datos a las autoridades. A futuro seguramente nuestro informe valorará los compromisos y acciones de las empresas en este sentido.

Adicionalmente, en Colombia, la virtualización de múltiples actividades por el Covid-19 supuso que quienes se encontraban en desventaja antes lo estuvieran más ahora, y evidenció la regresión en materia de derechos en distintos campos producto de la brecha digital.

La pandemia nos mostró cómo la tecnología que tiene el poder de impulsar el desarrollo y ampliar el ejercicio de los derechos para las personas, también puede incrementar las inequidades. Durante la pandemia, la acelerada digitalización de nuestras vidas mostró que la brecha digital se siente más en la ruralidad y afecta más profundamente a las personas en razón de su género, edad o autoreconocimiento en grupos minoritarios y étnicos, por ejemplo.

En los próximos años la capacidad de conectar y dar las mismas oportunidades con la tecnología a la población que habita la ruralidad será un factor central de las políticas públicas en una de las regiones más desiguales del mundo, América Latina, y por tanto para Colombia. Esperamos a futuro hacer eco de esta realidad en nuestro informe de manera articulada con nuestra revisión a los compromisos en derechos humanos de las empresas de telecomunicaciones.

¿Dónde están mis datos? Vistazo a nuestro informe

Como ha hecho cada año desde 2016 la Fundación Karisma publica nuevamente su informe "¿Dónde están mis datos?" con el que se propone analizar cómo las principales empresas proveedoras del servicio de internet y telefonía celular en Colombia dicen cumplir sus obligaciones en materia de derechos humanos. Se trata de un ejercicio que es replicado por otros países de la región y a nivel internacional por organizaciones especializadas en derechos humanos.[3]

Desde entonces, el objetivo de este informe ha sido proveer una herramienta que facilite a las personas usuarias el proceso de toma de decisión cuando contratan dichos servicios, y además ofrecer un instrumento que facilite la comprensión de aspectos de la tecnología que cada vez más deben ser de interés general para las personas.

"¿Dónde están mis datos?" analiza cómo protegen nuestros derechos a la libertad de expresión, intimidad y seguridad digital las siete compañías de internet y telefonía celular más importantes en el país: Claro, Movistar, Tigo, Etb, DirecTv, Emcali, Avantel. Como novedad en este informe que revisa la información disponible durante 2021, incluímos empresas de internet satelital como Hughesnet y Skynet por su rol para conectar a la ruralidad.

El informe evalúa lo que estas compañías *dicen hacer* a la hora de respetar el ejercicio de los derechos de las personas que usan sus servicios. No se pretende verificar si en efecto cumplen lo que dicen hacer.

En nuestra metodología[4] de análisis explicamos cómo desarrollamos dicho proceso, los cambios que efectuamos para evaluar el primer año de la pandemia, así como la información que consultamos en los dos ciclos de revisiones que llevamos a cabo y que socializamos previamente con las empresas evaluadas.

3 Nos referimos en concreto a los informes de la Electronic Frontier Foundation titulado "Who has your back?" y el informe anual de Ranking Digital Rights titulado "Corporate Accontability Index".

4 La metodología de análisis de 2020 se puede consultar acá. Los informes anteriores se pueden acceder https://web.karisma.org.co/pagina-principal/que-hacemos/investigaciones/demd/

Antes de adentrarnos a los cambios que introdujimos en nuestro informe queremos agradecer a las empresas que hicieron esfuerzos adicionales para atender las recomendaciones de nuestro informe en versiones anteriores, que apuntan, tal y como hemos sostenido en estos últimos seis años, a fortalecer conjuntamente el ejercicio de derechos en internet cuando se apoya en actores que juegan un rol determinante en su realización: los proveedores de acceso a internet.

Nuevo criterio general: Neutralidad de la red

Durante los primeros meses de la pandemia se impusieron cuarentenas estrictas en Colombia. La virtualidad obligada puso a prueba la capacidad de la infraestructura de la Red al tiempo que las autoridades elevaron llamados al consumo responsable y “productivo” de contenidos a tal punto en que diversos sectores elevaron inquietudes en torno a la probabilidad de su colapso[5].

Como resultado de los altos picos de tráfico en la navegación en esa época[6], el Gobierno Nacional así como la Comisión de Regulación de las Comunicaciones decidieron por medio de regulaciones de emergencia preparar el terreno en caso de que fuese necesario suspender la neutralidad de la Red.

En dichas regulaciones se previó la priorización de contenidos y servicios útiles para el teletrabajo, la educación virtual, y el acceso a servicios e información pública sobre la pandemia disponible en sitios web del Estado, sin que en ellos se haya resuelto la pregunta sobre por qué había que dejar de lado los contenidos de entretenimiento (vitales en términos de salud mental) o quién tendría a su cargo resolver los problemas derivados de dicha discriminación de contenidos en caso de que resultara arbitraria[7].

Pese a que dicho escenario -por suerte- no se llegó a concretar, entendimos que la neutralidad de la Red merecía ser un compromiso político objeto de evaluación en nuestro informe para aportar a las discusiones sobre su regulación y suspensión en futuros contextos de emergencia.

La neutralidad de la Red es una garantía que asegura que el tráfico de Internet sea tratado sin discriminar por el tipo de dispositivo o contenido que se crea, accede o consulta por condiciones orientadas en su tipo, origen, geografía, autor, etc.[8]. Su protección, en resumidas cuentas, “es fundamental para garantizar la pluralidad y diversidad del flujo informativo” en la gran red de redes[9].

Si bien es cierto que dicha garantía puede ser limitada en casos excepcionales previa satisfacción de criterios de proporcionalidad, razonabilidad, necesidad y legalidad; también lo es que regular sobre dichos escenarios precisa, al tiempo, del continuo fortalecimiento de los mecanismos de transparencia que deben ser implementados por las empresas proveedoras del servicio de internet (PSI).

---

5 Ver por ejemplo la columna de Carolina Botero, directora de Fundación Karisma, en El Espectador https://elespectador-el-espectador-sandbox.cdn.arcpublishing.com/opinion/columnistas/carolina-botero-cabrera-sand/el-autocontrol-para-que-internet-no-colapse-requiere-de-mas-informacion-column-912694/ ; la noticia publicada en Revista Semana sobre los riesgos de eventual colapso de internet por “avalancha del teletrabajo” https://www.semana.com/economia/articulo/capacidad-de-conexion-a-internet-de-colombia-para-facilitar-el-teletrabajo/657315/ ; o la columna de Camilo Andrés Garzón en la Silla Vacía sobre el mismo tema https://www.lasillavacia.com/historias/silla-nacional/hay-una-colombia-para-la-cual-internet-no-es-una-alternativa-frente-al-coronavirus/

6 La Comisión de Regulación de las Comunicaciones publica desde abril de 2020 informes sobre el comportamiento del tráfico de la Red con información que proveen los PSI con más de 50.000 usuarios. Pueden accederse aquí https://www.crcom.gov.co/es/noticias/estudio/reporte-trafico-internet-durante-emergencia-sanitaria-declarada-por-ministerio

7 Ver el análisis que hicimos en el marco del Índice Derechos Digitales sobre el Decreto 464 de 2020 aquí https://cv19.karisma.org.co/docs/Decreto464MinisterioTIC/

8 Ver el informe que publicó Fundación Karisma sobre neutralidad de la Red en 2017 aquí.

9 Comisión Interamericana de Derechos Humanos (2013). Informe “Libertad de Expresión e Internet”. Ver aquí https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf pg. 28

Para integrar este compromiso en nuestro informe decidimos partir del deber legal[10] que ordena a los PSI la publicación de sus Prácticas de Gestión del Tráfico, es decir, las reglas *razonables y no discriminatorias* que deben aplicar a la hora de garantizar un mejor servicio, y que en su aplicación no debe reñir con la garantía de neutralidad de la Red cuya normativa de base se remonta a 2011.

En adelante, verificaremos que las empresas publiquen este tipo de información que, esperamos, esté redactada de manera fácil y "en un formato que resulte accesible para todos los interesados"[11].

Nuevo criterio general: acceso directo

En Colombia no contamos con un marco legal que desarrolle con detalle la figura según la cual las autoridades públicas pueden acceder de manera directa a la infraestructura y datos de las telecomunicaciones de las personas eliminando de la ecuación a los proveedores de acceso a internet. Esta situación, conocida internacionalmente con el nombre de *acceso directo*[12], es una forma de vigilancia masiva de las comunicaciones que permite a las autoridades interceptar las comunicaciones personales sin necesidad de que intervengan las empresas que prestan dichos servicios.

En Colombia, las autoridades acceden a las comunicaciones de las personas usuarias de las empresas que ofrecen dicho servicio a través de una puerta abierta a su infraestructura de telecomunicaciones contando además con la tecnología que les facilita dicho acceso[13].

¿Cómo sabemos que en Colombia las autoridades acceden directamente a los datos de las telecomunicaciones de las personas suscriptoras de estos servicios? Aunque no hay suficiente claridad en el marco legal aplicable, las autoridades se han apoyado en disposiciones del Decreto 1704 de 2012 para implementar el acceso directo e interceptar las comunicaciones sin intervención de la empresa que tiene las redes.

Es poco lo que sabemos sobre cómo sucede esta actividad pero, en el seguimiento que Karisma ha efectuado a través de *¿Dónde están mis datos?*, hemos visto que algunas empresas desde 2017 han documentado su existencia en sus informes de transparencia (caso de Movistar, Claro y Tigo) al sugerir o indicar expresamente una diferencia entre la interceptación de las comunicaciones sobre telefonía fija que dista de la interceptación sobre la telefonía celular.

El informe de transparencia de Movistar desde 2017 (y que mantiene en 2020) indica que "[n]o se reportan interceptaciones sobre líneas móviles: La Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptaciones de manera directa sobre las líneas móviles"[14]. Claro, por su parte, solo indica que hay una diferencia en el marco legal aplicable, mientras que Tigo ha hecho más explícita la información que da cuenta de esa realidad.

Desde Karisma seguimos animando a las empresas a dar más información sobre la interceptación de

10 Resolución 3502 de 2011, art. 7

11 Comunicado de Prensa sobre el Comunicado conjunto de las Relatorías de Libertad de Expresión acerca de Internet, ver https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=848 apartado 5 (b).

12 Estas normas se han adoptado en diferentes jurisdicciones y han despertado importantes críticas incluso del sector privado de proveedores de internet como lo muestra la declaración de la empresa noruega Telia que puede leerse aquí https://www.teliacompany.com/en/news/news-articles/2019/respecting-freedom-of-expression--telia-companys-view-on-new-surveillance-law-direct-access-in-norway/

13 La Fundación Karisma hizo una traducción del comunicado de GNI sobre el acceso directo y que puede leerse aquí https://web.karisma.org.co/definiendo-el-acceso-directo-gni-hace-un-llamado-por-una-mayor-transparencia-y-dialogo-en-torno-al-acceso-de-los-datos-de-las-personas-usuarias-de-los-servicios-de-telecomunicaciones-por-parte-de-los/

14 El informe de transparencia puede consultarse aquí https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf

las comunicaciones que efectúa las autoridades. Con el fin de aportar más datos que permitan a las personas entender mejor esta modalidad de vigilancia de comunicaciones, a partir de 2021 el informe evaluará a los proveedores del servicio de internet que de manera clara y accesible cuenten a sus suscriptores sobre la existencia del acceso directo, que permitan entender cómo sucede respecto a las investigaciones criminales y de inteligencia, y cuál es el marco jurídico que soporta esta acción.

Nuestra meta a futuro es poder dar luz sobre una situación que la *Global Network Initiative* (GNI por sus siglas en inglés, una organización que reúne a cientos de empresas de telecomunicaciones con organizaciones de la sociedad civil, academia e inversionistas para enfrentar los desafíos en materia de libertad de expresión y derechos humanos alrededor del mundo) ha manifestado como preocupante por la falta de transparencia de los Estados en torno a su uso, y por su incremento progresivo en distintos países como fruto del covid-19[15].

Cambios adicionales al informe

Un par de cambios adicionales se verán reflejados en esta evaluación del primer año de pandemia.

Se trata, por un lado, de la inclusión de un nuevo evento de bloqueo de URL y contenidos en los ejes de transparencia y libertad de expresión en los que verificaremos que se provea información sobre solicitudes motivadas en los casos de emergencia sanitaria y estados de excepción.

En concreto, buscamos que los PSI provean información accesible y clara sobre cuántos bloqueos han efectuado por motivo de la pandemia (un caso de emergencia y excepción todavía vigente), pues nos interesa empezar a documentar cómo evoluciona el número de solicitudes de este tipo, particularmente porque vimos órdenes de bloqueos o retiro de publicaciones soportados en posibles noticias falsas sobre el covid-19 o la difusión de publicidad engañosa en internet sobre curas milagrosas[16].

Por otro lado, incluimos nuevos actores: las empresas de internet satelital (Hughesnet y Skynet). Evaluar sus compromisos en materia de transparencia, libertad de expresión, intimidad y seguridad digital cobra relevancia en tanto que se trata de PSI cuya cobertura regional es significativa y cada vez mayor. Por ejemplo, Skynet es una empresa que provee servicios de conectividad en más de 1.100 municipios en 32 departamentos de Colombia[17]. Hughesnet es un proveedor con cobertura en al menos 1.000 municipios repartidos en 20 departamentos según uno de sus informes más recientes[18].

Creemos que las personas que decidan contratar sus servicios merecen conocer cuáles son las políticas con las que estas compañías dicen respaldar sus prácticas en la prestación de un servicio que hoy en día la legislación colombiana considera como uno de tipo esencial y universal.[19]

---

15 Publicación original que puede consultarse aquí https://globalnetworkinitiative.org/defining-direct-access-2/

16 Como las órdenes de la Superintendencia de Industria y Comercio para que influencers (caso Natalia París https://www.sic.gov.co/slider/superindustria-ordena-natalia-par%C3%ADs-el-cese-inmediato-de-la-promoci%C3%B3n-del-producto-di%C3%B3xido-de-cloro y Elizabeth Loaiza https://www.sic.gov.co/slider/superindustria-sanciona-elizabeth-loaiza-junca-por-publicidad-enganosa-al-promocionar-pruebas-rapidas-de-covid-19) retiren publicidad engañosa sobre el covid-19. Una situación que el Índice Derechos Digitales, del cual Karisma hace parte, analizó en el pasado https://indicecoronavirus.digital/docs/OrdenRetirarContenidosSIC/

17 Ver su sitio web https://www.sky.net.co/

18 Ver la entrada en su blog titulada "El internet satelital está conectando al campo colombiano", disponible aquí.

19 Ley 2108 de 2021

Principales hallazgos

Tal y como anunciamos más atrás, en esta versión integramos nuevos actores, Hughesnet y Skynet. Sobre las demás compañías proveeremos un comparativo sobre su desempeño, no sin antes dejar de recordar que nuestra evaluación se orienta en la revisión del contenido de políticas, documentos y compromisos públicos que se encuentran disponibles en los sitios web de cada proveedor de acceso a internet. La metodología no permite establecer si los compromisos se cumplen.

En la edición de este año al tiempo que evaluaremos a los PSI, mencionaremos casos que documentamos durante el primer año de pandemia y que justificaría la implementación progresiva de mejoras en dichas políticas y documentos en aras de garantizar plenamente los derechos de las personas suscriptoras de sus servicios. Dicha documentación la incluiremos, cuando aplique, en una sección de *contexto e interés.*

1. Eje de compromisos políticos

1.1. Políticas de género y políticas de accesibilidad

Buscamos incentivar a los PSI a través de nuestro informe para que incluyan buenas prácticas sensibles y respetuosas en materia de género, incentiven y promuevan la diversidad y la accesibilidad que permita integrar a personas con capacidades diversas tanto en el marco de sus operaciones internas como en la oferta de sus servicios comerciales. Consideramos que una empresa que tenga diversidad y sensibilidad por estos temas puede desarrollar políticas y prácticas más inclusivas y garantistas de la tecnología.

En dicha evaluación verificamos si, por ejemplo, cuentan con políticas sobre selección y contratación de su personal que activamente promueva la selección de mujeres así como de poblaciones y comunidades minoritarias y diversas en el sector de las Tecnologías de la Información y las Comunicaciones (TIC). Si cuentan con políticas de desarrollo de carreras y capacitación de su personal, si cuentan con políticas favorables al equilibrio familiar y laboral, así como políticas dedicadas a prevenir y gestionar casos de abuso y acoso sexual en el trabajo, y la promoción de imágenes publicitarias no sexistas.

En materia de accesibilidad buscamos identificar políticas que explícitamente declaren el compromiso del PSI por promover ajustes razonables y que integren especialmente a las personas con discapacidad y les permita el acceso y consulta de los contenidos que publican estas compañías en sus sitios web.

En materia de género y accesibilidad destacan particularmente **Movistar** y **Tigo**, seguidos de **Claro**, **ETB** y **DirecTV** que comparten un puntaje similar.

Movistar y **Tigo** publican diversas políticas que abordan por completo los ítems evaluados. Y si bien

Tigo no cuenta con una política de accesibilidad, recibió puntaje favorable por hacer disponible en su sitio web los ajustes razonables que permitirán en adelante a las personas usuarias de sus servicios acceder a los contenidos en alto contraste, con ajustes en el tamaño de letra, entre otros.

Nos parece igualmente relevante destacar el caso de **DirecTV.** Desde su adquisición en 2021 por el Grupo Werthein basado en Argentina, ha publicado información sobre políticas sensibles en materia de género y diversidad que especifican, por ejemplo, el diseño de planes de trabajo para ampliar la representación de grupos LGBTI, de personas con discapacidad y mujeres tanto en sus operaciones como en su comunidad de personas usuarias. Esta nueva realidad empresarial seguro les permitirá recibir un puntaje más destacado en ediciones futuras de nuestro informe.

1.2. Informes de transparencia

1.2.1 Solicitudes de datos del suscriptor, bloqueos de URL, interceptaciones de las telecomunicaciones

La ley colombiana no obliga a los operadores a presentar informes de transparencia o informes periódicos sobre los requerimientos que las autoridades hacen de los datos de las personas que usan sus servicios. Sí tienen obligación de entregar información pero sobre los planes de internet y telefonía celular o las prácticas de gestión de tráfico. Sin embargo, dar información sobre lo que sucede con los datos que recolectan se ha convertido en una buena práctica internacional especialmente entre las empresas del sector de las TIC.

Ahora bien, como responsables del tratamiento de datos personales, los PSI sí tienen obligaciones de informar con claridad qué datos recogen y cómo los usan, así como de tener una política de tratamiento de datos que advierta los eventos en que debe entregar los datos de sus suscriptores al Estado[20].

En esta evaluación nos interesan tres tipos de peticiones o solicitudes que pueden elevar las entidades del Estado a los proveedores de internet y telefonía celular que son: (i) la entrega de datos de las personas suscriptoras[21], (ii) las solicitudes de interceptaciones a líneas telefónicas fijas[22] y (iii) los bloqueos de URL o sitios web motivadas, a su vez, en cuatro subtipos: la prevención del abuso sexual infantil en línea[23], combatir la ilegalidad en los juegos de suerte y azar[24], las órdenes de tipo judicial y administrativas, y las emitidas en el marco de los estados de emergencia y excepción[25].

Ante estos tres tipos de solicitudes que impactan en la privacidad y libertad de expresión de las personas usuarias de las empresas, esperamos que éstas, de manera pública y accesible, relacionen el número de solicitudes recibidas por mes o año, las autoridades que efectúan estos pedidos, así como la relación de cuáles y cuántas solicitudes fueron atendidas de manera favorable y cuál terminó siendo su extensión en el tiempo.

20 Obligaciones que se encuentran enmacadas por la Ley 1581 de 2012 y el decreto 1377 de 2013 especialmente.

21 Art. 15 de la Constitución, Ley Estatutaria 1266 de 2008, Ley 1581 de 2012, Art. 244 de la Ley 906 de 2004 (búsqueda selectiva en bases de datos), modificado por la Ley 1908 de 2018; numeral 9 del Art. 277 de la Constitución Política (solicitud del Procurador General de la Nación); Arts. 631 y 684 del Estatuto Tributario (DIAN) y Cobro Coactivo de entidades públicas (Ley 1066 de 2006). Art. 44 de la Ley Estatutaria 1621 de 2013 (inteligencia y contrainteligencia); Art. 4 del Decreto 1704 de 2012 (interceptación legal).

22 Art. 1 del Decreto 1704 de 2012.

23 Según lo contenido en el art 7 y art 8 de la Ley 679 de 2001; art. 5 y art. 6 del Decreto 1524 de 2002.

24 Según lo ordena el art. 38 de la Ley 643 de 2001.

25 Según el art. 8 de la Ley 1341 de 2009.

En 2021, **Movistar** sigue siendo la empresa con el mejor puntaje. Informa de manera plena sobre todos los criterios esperados y de forma desagregada, incluyendo los eventos de bloqueo ante la declaración de estados de emergencia o excepción. **Claro** y **Tigo** compiten con un mismo puntaje en este eje.

Claro informa sobre la ocurrencia de cada evento, el marco legal en que se justifica cada orden, las autoridades con facultad para elevarlas ante la compañía, pero a la hora de proveer estadísticas desagregadas sólo lo hace en relación con las órdenes de bloqueo y los cuatro subtipos en que ésta se puede justificar.

Tigo mejoró en comparación con el año anterior. En 2021 la empresa entregó información sobre las órdenes de bloqueo de URL o sitios web, así como de solicitudes de datos personales de sus suscriptores, incluso éste último evento lo desagrega con especial detalle al especificar la autoridad requirente, el tipo de datos requeridos, y las solicitudes recibidas vs las solicitudes atendidas.

ETB retomó para 2021 su informe de "transparencia de datos". Allí relaciona información desagregada sobre las solicitudes de datos del suscriptor así como las órdenes de bloqueo de URL o sitios web que fueron recibidas, desagregando en ambos eventos por autoridad solicitante, y por solicitudes procedentes vs las solicitudes recibidas.

En este primer año de pandemia compañías como **DirecTV**, **EmCali**, **Avantel** y **Skynet** no publicaron informes de transparencia con información que permitiese evaluar su desempeño en este eje.

DirecTV sigue publicando el procedimiento de bloqueo que se refiere en exclusivo a contenido asociado con el abuso sexual infantil. Tomamos nota de su adquisición reciente por un grupo empresarial argentino, lo que puede que permita generar avances en materia de transparencia como los que ya se han documentado positivamente en políticas de género y accesibilidad.

Hughesnet no cuenta con un informe de transparencia o sostenibilidad, pero en su política de tratamiento de datos informa que efectúa procesos de 'filtrado' de contenidos de abuso sexual infantil.

De contexto e interés

Compañías como **Claro**, **Tigo** y **ETB** no relacionan información sobre el número de solicitudes recibidas dirigidas a la interceptación de las telecomunicaciones de sus suscriptores. Movistar en su informe de transparencia señala que han cursado cero solicitudes de interceptación durante 2017, 2019 y 2020. Y que en 2018 recibió apenas 2 solicitudes de este tipo.

Movistar de nuevo señala que sobre la interceptación de líneas móviles no se reportan datos pues "la Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptación de manera directa sobre las líneas móviles".

La ausencia de solicitudes de interceptación de comunicaciones para líneas fijas confirma no solo que predominan las comunicaciones por vía celular, sino que es un indicio que permite entender por qué las autoridades han acudido cada vez menos al mecanismo tradicional de interceptación de comunicaciones vía los PSI (y que estos documentan en sus informes de transparencia cada vez menos) acudiendo en su lugar al acceso directo. Sobre esto ahondaremos en la sección sobre acceso directo en el eje de intimidad.

1.2.2. Neutralidad de la Red

La neutralidad de la Red es una garantía que desde 2011 se encuentra regulada en Colombia[26]. Tal y

26 Ver la Ley 1450 de 2011, y la Resolución 3502 de 2011.

como lo describimos en nuestro informe sobre el tema, la neutralidad de la Red impone una prohibición a los proveedores del servicio de internet de "no interferir en el uso que las personas hacen de internet, siempre que este uso sea legal"[27].

Dicha prohibición se articula a través de cuatro principios: libre elección, no discriminación, transparencia e información[28].

El primero reconoce en cabeza de las personas usuarias de los servicios de telecomunicaciones el derecho a utilizar, enviar, recibir u ofrecer cualquier contenido y servicio en línea a través, además, de cualquier tipo de tecnología digital. Y se prohíbe a los PSI su limitación arbitraria. El segundo, asegura que los PSI brindarán un trato igualitario a los contenidos y aplicaciones sin diferenciar en razón del contenido, su autor, origen, formato, etc. El tercero obliga a los PSI a proveer información sobre sus políticas de gestión del tráfico. Y el cuarto reconoce el deber de las compañías de internet de suministrar información sobre las condiciones de prestación del servicio en términos de velocidad, calidad, prácticas de gestión del tráfico según el plan de navegación, entre otros[29].

Las Prácticas de Gestión del Tráfico (PGT) a través de las cuales los PSI pueden intervenir en el tráfico de internet para "reducir o mitigar los efectos de la congestión sobre la red" o "asegurar la calidad del servicio a los usuarios", entre otros, deben ser razonables y no discriminatorias.

En nuestra evaluación consultamos el contenido de las PGT y observamos que todos los PSI (a excepción de **Skynet**) las publican en sus sitios web, con alguna variación en términos de claridad y facilidad en su búsqueda.

Destacamos particularmente los casos de **Movistar**, **Tigo**, **Avantel** y **Hughesnet** que además de publicar sus prácticas de gestión del tráfico hacen expreso su compromiso por proteger el principio de neutralidad de la red.

De contexto e interés

En 2020 el gobierno nacional expidió dos decretos[30] que previeron la posibilidad de priorizar el tráfico de internet en caso de que fuese necesario para privilegiar la navegación de contenidos sobre "servicios de salud, páginas gubernamentales y del sector público, el desarrollo de actividades laborales".

Su desarrollo a nivel infralegal se desprendió en ese mismo sentido por la Comisión de Regulación de las Comunicaciones[31] que expresó que la priorización podría versar sobre "aplicaciones y contenidos de salud, gobierno, sector público, actividades laborales, educación, y derechos fundamentales"[32].

Antes de su aplicación, según lo estableció la CRC, los PSI debían informar previamente a la autoridad de las comunicaciones sobre la evidencia disponible que justificara acudir a dicha medida de priorización. Además, impuso a su cargo el envío periódico de información sobre el comportamiento del tráfico

27 Fundación Karisma (2017). *Neutralidad de la red y ofertas comerciales en Colombia. Análisis de la regulación*. Ver https://web.karisma.org.co/fundacion-karisma-publica-informe-sobre-neutralidad-de-la-red-en-colombia/ pg. 8

28 Art. 3 Resolución 3502 de 2011

29 Art. 3 Resolución 3502 de 2011

30 Decreto 464 de 2020 renovado en el tiempo por el Decreto 555 de 2020.

31 Integrado por la Resolución 5951 de 2020 (derogada), Resolución 5969 de 2020. Hicimos un análisis de esta última resolución para el Índice Derechos Digitales que se encuentra disponible aquí https://indicecoronavirus.digital/docs/Resolucion-5969CRC/

32 Art. 2, Resolución 5969 de 2020.

de internet, destinado a informar sobre el estado de la Red y los picos de mayor demanda del servicio, así como orientar la toma de decisiones sobre posibles eventos en que hubiese sido necesario aplicar dicha medida.

El impacto de la misma pretendió ser extendido a futuro a toda "ocurrencia de pandemias declaradas por la Organización Mundial de la Salud". La revisión constitucional del decreto 464 y 555 sirvió como escenario para que Karisma junto con otras organizaciones formulara comentarios[33] en torno a la desproporción de una medida de este tipo con efectos a futuras emergencias sanitarias. También se enfatizó en que toda suspensión del principio de neutralidad, sea parcial o total, debía acompañarse por la aplicación de estándares más elevados en materia de transparencia y publicidad correlativa de la información. Se trató de una postura compartida igualmente por la Procuraduría General de la Nación que intervino en dicho proceso.

El fallo[34] de la Corte Constitucional recogió dichas preocupaciones y aclaró que la previsión sobre la priorización del tráfico no significaba instaurar en la práctica un mecanismo de bloqueo de contenidos. Y pese a que no consideró que hubiese ninguna afectación arbitraria sobre el principio de neutralidad de la Red, acogió la postura según la cual la información producida por los PSI debía ser transparente, no podía ser calificada como reservada, y su acceso debía ser público, libre y accesible.

Esta decisión fue particularmente rica por cómo en sus votos separados algunos magistrados de la Corte Constitucional permitieron recuperar interés en un principio tan importante para Internet. Algunos magistrados decidieron en sus salvamentos de voto ahondar especialmente en la importancia de la neutralidad de la Red y las precauciones que deben tomarse para su limitación parcial.

Una de las magistradas ponentes refirió incluso a cómo los decretos que consagran estas medidas de priorización podían habilitar al despliegue de técnicas como la inspección profunda de paquetes[35] (postura que puede o no ser compartida). Otra magistrada sostuvo que la Corte debió haber introducido condiciones más estrictas para que las medidas de priorización del tráfico fuesen verdaderamente excepcionales[36]. Pese a las direcciones que tomó el debate constitucional éste contribuye, en todo caso, a enriquecer dogmáticamente y actualizar el interés sobre esta materia.

2. Eje de intimidad

2.1. Políticas de protección de datos

La ley de protección de datos obliga al responsable de su tratamiento a contar con una política que permita advertir al titular qué información personal y sensible suya será recabada, para qué fines, qué uso se dará a los mismos y si se compartirá dicha información con terceros. Dicha política debe poder estar publicada y ser accesible para las personas suscriptoras a los servicios de los PSI.

33 Suscritos también por la Fundación para la Libertad de Prensa, el Centro de Estudios de Internet y Sociedad de la Universidad del Rosario ISUR, y Emmanuel Vargas Penagos. Puede leerse aquí https://web.karisma.org.co/intervencion-de-la-corte-decreto-417-2020/

34 Que puede verse aquí https://www.corteconstitucional.gov.co/relatoria/2020/C-151-20.htm

35 Ver el salvamento de voto de la magistrada Gloria Stella Ortiz Delgado. Su voto luego fue reiterado en el mismo sentido en el fallo C-209 de 2020 que analizó la constitucionalidad del Decreto 555 de 2020 cuyo contenido es idéntico al del Decreto 464 de 2020.

36 Ver el salvamento de voto de la magistrada Diana Fajardo Rivera.

Ya en los últimos informes habíamos mencionado cómo la confección de las políticas de protección de datos por parte de los PSI han dado un salto significativo en comparación con la primera evaluación de *¿Dónde Están mis Datos?* de 2015. Pese a que ha habido progresos sustanciales en esta materia, creemos que todavía se requiere de un mayor nivel de desagregación y granularidad en la información que se provee sobre los datos objeto de tratamiento y su compartición con terceras partes (del sector público y privado).

En comparación con los hallazgos del año anterior no se produjeron cambios[37], por tanto **Claro**, **Movistar, Tigo**, **ETB**, **Emcal**i, **Avantel** y **DirecTV** recibieron el mismo puntaje dada la ausencia de modificaciones en sus políticas de tratamiento de datos.

Hughesnet cuenta con una política pública en su sitio web en la que advierte qué información personal habrá de recoger de sus suscriptores: nombre, dirección, estrato, número telefónico, dirección de correo electrónico y su información financiera, tal como la información de su tarjeta de crédito. Describe así mismo hasta veintisiete tipos de finalidades distintas en las que se justifica la recolección de dicha información, pese a que no describe qué terceros podrán tener acceso a éstos y en dicho caso para satisfacer qué finalidad en concreto.

Por su parte, **Skynet** informa las diez finalidades que justifican el tratamiento de datos personales de sus suscriptores, pero no define qué datos son esos más allá de advertir que son "datos personales". Tampoco señala si comparte o no dichos datos con terceros y en caso afirmativo, para qué fines en concreto.

Este año **Avantel** mantuvo en su política de protección de datos una estrategia que sugerimos en nuestro informe anterior que valdría la pena replicar. Creemos que otros PSI puedan observar de cerca y adoptarla para ampliar el conjunto de buenas prácticas en la materia. La compañía consagra un análisis de impacto en privacidad para evaluar la compatibilidad de prácticas de protección de datos con las políticas institucionales, y el derecho de supervisar de manera periódica el cumplimiento de los requisitos legales y contractuales asociados al régimen de protección de datos personales por parte de terceros con los que la compañía sostiene un vínculo comercial.

2.2. Retención de datos

Cuando hablamos de retención de datos nos referimos específicamente a la obligación que tienen los PSI de conservar hasta por cinco años y entregar de manera *inmediata* a las autoridades de inteligencia y a la Fiscalía General, la información que producen en la prestación del servicio de telecomunicaciones.

En dicho caso, las compañías de telecomunicaciones deben colaborar con la Fiscalía General de la Nación para entregar, en el marco de una investigación penal, los siguientes datos[38]:

- Los datos de la persona suscriptora, tales como identidad, dirección de facturación y tipo de conexión. Además deben conservarla por cinco años.
- Información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación. Deben suministrarla en tiempo real en caso de que se requiera.

37 Puede verse aquí https://web.karisma.org.co/donde-estan-mis-datos-2020/

38 Decreto 1704 de 2012, artículo 4.

La ley de Inteligencia y contrainteligencia obliga a los operadores a entregar a agencias de inteligencia[39]:

- El historial de comunicaciones de los abonados telefónicos vinculados, es decir, de las personas que contratan sus servicios.
- Los datos técnicos de identificación de las personas que suscriben sus servicios y sobre los que recae su operación,
- La localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización.

Sin embargo, de toda la información que pueden producir los operadores sobre la actividad de los teléfonos celulares, no está claro exactamente qué entregan a las autoridades de investigación penal e inteligencia cuando deben cumplir con estas normas. Por eso, en esta pregunta nos preocupamos por cómo informan (i) a las personas usuarias sobre la existencia de esta obligación, (ii) sobre qué datos retienen en concreto, (iii) sobre el tiempo por el cual los retienen.

Además de las normas de retención de datos que acabamos de exponer, la Fiscalía puede realizar la "búsqueda selectiva en bases de datos"[40] y las autoridades, en general, pueden solicitar datos personales sin autorización del titular, siempre que sea en ejercicio de sus funciones[41]. No está claro cómo funcionan en la práctica cada una de estas facultades ni cómo se relacionan entre ellas.

En esta sección revisamos la forma como los operadores informan que desarrollan su obligación de retención de datos, cuáles son los que retienen y por cuánto tiempo. No revisamos el resultado de la actividad de retención de datos. Por ejemplo, el tipo de datos de las personas usuarias que fueron entregados en efecto a la Fiscalía.

Para esta edición nuevamente la mayoría de los operadores informan sobre el cumplimiento de la ley -con o sin la indicación del marco legal al que hacen referencia-, o publican que deben retener los datos de las personas que se suscriben a sus servicios.

Sobre los datos que conservan para entregar a las autoridades en investigaciones penales o de inteligencia o el tiempo que dura la retención, los operadores no introdujeron cambios en 2021 en comparación con la información que ya proveían para 2020. En general las empresas en Colombia no son claras en los detalles en torno al cumplimiento de esta obligación legal. Veamos.

Claro, **Movistar** y **Tigo** informan que están obligadas por ley a retener datos en indicación del marco legal. **ETB** menciona en su política de tratamiento de datos que retiene datos sin indicación del marco legal.

Claro vuelve a ser la única que advierte el tiempo por el que retiene datos, el cual se extiende hasta por 10 años, al parecer tomando el plazo de retención de los archivos de tipo contable sin que se explique cómo difrencia este plazo del que la ley ordena para la retención de datos para investigaciones penales y de inteligencia que es solo de 5 años.

Movistar cita a plenitud el marco legal que justifica la retención de datos. Incluyen la Ley 906 de 2004 (art. 235), Ley 1621 de 2013 (art. 44), y el Decreto 1704 de 2012 (art. 18). Ese marco legal describe el tiempo de retención que se extiende hasta por cinco años, el tipo de datos que son retenidos (metada-

39 Ley 1621 de 2013, artículo 44.

40 Ley 906 de 2004. Código de Procedimiento Penal. Artículo 244.

41 Ley 1581 de 2012. Artículos 10 y 13.

tos como el historial de comunicaciones de las personas que suscriben sus servicios, su identificación, datos que faciliten su localización, entre otros).

Tigo por su parte informa que tiene un deber legal de retención de datos sin especificar el marco legal en que se funda ese deber. Cuando se trata de detallar el tiempo por el que hace la retención de dichos datos, señala que lo hará por un periodo superior al autorizado por la persona titular de los datos sin la advertencia de un plazo determinado en el tiempo.

ETB emplea una fórmula más bien genérica para señalar, por ejemplo, que retendrá los datos por el tiempo que sea necesario hacerlo.

Por último, **DirecTV**, E**mCali**, **Avantel**, **Hughesnet** ni **Skynet** relacionan información sobre el deber legal de retención de datos, sobre el tipo de datos que retienen, ni el tiempo por el que lo hacen.

2.3. Acceso directo

Los estándares internacionales de derechos humanos obligan a que la interceptación de las comunicaciones requiera por mandato legal que una autoridad competente emita una orden que está sujeta a parámetros estrictos de motivación fundada y razonable, y que en su confección atienda además un test de proporcionalidad en el que se justifique el qué, para qué y por cuánto tiempo de una medida que impacta en la privacidad de las personas.

Dicha orden de acceso a las comunicaciones se remite a los proveedores de servicios de internet que pueden validar y analizar su contenido y forma y, en caso de hallarla deficiente o arbitraria, pueden oponerse a su ejecución. La intermediación le da a estas empresas un rol en la garantía de los derechos fundamentales de las personas que contratan sus servicios.

El acceso directo, por su parte, faculta a las autoridades a tener acceso a las comunicaciones de las personas prescindiendo del rol de los PSI, situación que se ve aunada a su desregulación o ambigüedad legal que no cumplen con los estándares internacionales de protección a los derechos humanos. En el acceso directo las empresas están obligadas a dejar una puerta abierta en su infraestructura sin que tengan capacidad de negarse (puede llegar a ser una condición para funcionar en determinados países[42]), o de denunciarlo públicamente, tal y como lo han manifestado algunos proveedores internacionales de acceso a internet como Vodafone, Telenor, Millicom (antiguo propietario de DirecTV) y Telia[43].

Al tiempo que algunos proveedores del servicio de internet han arrojado alguna luz sobre este tipo de prácticas a través de sus informes de transparencia, y han acusado su incompatibilidad con estándares en materia de transparencia, privacidad y libertad de expresión; han decidido al tiempo reclamar por cómo el acceso directo significa perder dominio y control sobre su propia infraestructura[44].

El Tribunal Europeo de Derechos Humanos tuvo la oportunidad de referirse al acceso directo en el fallo

---

42 Ver la publicación de Katitza Rodríguez y Veridiana Alimonti en el Blog de la Electronic Frontier Foundation en donde se recoge un extracto a la explicación de Telecom sobre por qué no puede oponerse al acceso directo "some governments may require direct access into companies' infrastructure for the purpose of intercepting communications and/or accessing communications-related data. This can leave the company without any operational or technical control of its technology". Ver aquí https://www.eff.org/deeplinks/2021/02/when-law-enforcement-wants-your-private-communications-what-legal-safeguards-are

43 En el blog de la Freedom Online Coalition tanto Lisl Brunner y Patrick Hiselius informan en detalle al respecto. La entrada puede consultarse aquí https://freedomonlinecoalition.com/blog/blog-2-direct-access-systems-and-the-right-to-privacy-by-lisl-brunner-and-patrik-hiselius/

44 *Idem.*

de Roman Zakharov v. Rusia[45], proferido en 2015. En dicho fallo el Tribunal sentenció que el acceso directo es una práctica propensa al abuso[46], y que la orden de una autoridad estatal en la que constan los fundamentos de la intención de acceder a los datos de las comunicaciones de una persona son la garantía más importante para asegurar la aplicación de la ley y el respeto de sus derechos[47]. El demandante del caso remarcó también que el acceso directo permitía la interceptación indiscriminada de las comunicaciones[48]. Además de su legalidad, esto pone en cuestión la necesidad y proporcionalidad de la práctica de acceso directo. Una práctica que permite la vigilancia indiscriminada de las comunicaciones va en contra de los estándares internacionales de derechos humanos.

Tal y como lo puso de presente la organización Privacy International en su intervención[49] ante el Relator Especial para la Libertad de Expresión de la ONU a propósito de las prácticas de acceso directo que estaban siendo documentadas y denunciadas en la Antigua República Yugoslava de Macedonia en 2016, el acceso directo no es una práctica reciente. Se viene documentando su uso en diversos países del mundo desde los años 90.

Privacy International destacó en su informe el valor que tienen los informes de transparencia de las compañías proveedoras de acceso a internet para visibilizar este tipo de prácticas en los casos en que no pueden denunciar públicamente su despliegue. Es más, recoge casos de los informes de empresas que han permitido en varias partes del mundo identificar en qué países se ejecutan actividades de acceso directo sin supervisión ni control legal.

Más recientemente, durante la pandemia, la GNI[50] se manifestó en torno a este tipo de prácticas al decir que:

> **Cuando los datos son extraídos a través del acceso directo se pueden utilizar para acusar, detener, condenar o encarcelar a personas, situación** *que podría infringir el derecho a la libertad, la seguridad de la persona y el debido proceso.* **En términos más generales,** *los Estados que recurren al acceso directo probablemente debilitan la confianza pública tanto en la responsabilidad del gobierno como en la fiabilidad y seguridad de las tecnologías de las comunicaciones.* **Este abuso de confianza puede llevar a consecuencias masivas y dañinas de tipo político, social y económico[51] (Subrayado nuestro).**

En Colombia, el Decreto 1704 de 2012 sobre interceptación de las comunicaciones prevé que "[l]os proveedores de redes y servicios de telecomunicaciones (...) deberán implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión *y de acceso* a la captura del tráfico de las comunicaciones que cursen por sus redes". Aunque esta no es una previsión lo suficientemente precisa como para responder a la pregunta sobre si esta práctica se encuentra o no consagrada, se menciona por algunos PSI colombianos como la base legal de despliegue de este mecanismo de vigilancia de las comunicaciones.

Con esta nueva edición de nuestro informe hemos decidido emprender la tarea de documentar y poner especial atención a lo que informan los PSI al respecto. Empezamos con las afirmaciones que algunas de

---

45 Puede leerse el fallo aquí https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}

46 *Idem*, párrafo 270.

47 *Idem*, párrafo 269.

48 *Idem*, párrafo 160.

49 Se puede leer acá https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/PrivacyInternational.pdf

50 Publicación original que puede consultarse aquí https://globalnetworkinitiative.org/defining-direct-access-2/

51 Traducción de la publicación de GNI efectuada por la Fundación Karisma. Disponible en español aquí https://web.karisma.org.co/definiendo-el-acceso-directo-gni-hace-un-llamado-por-una-mayor-transparencia-y-dialogo-en-torno-al-acceso-de-los-datos-de-las-personas-usuarias-de-los-servicios-de-telecomunicaciones-por-parte-de-los/

las empresas han hecho desde 2017 y sobre todo los datos más recientes de Movistar en su informe de 2020 en donde es claro que las empresas no pueden documentar las interceptaciones de líneas móviles en tanto que se trata de una actividad que ejecuta de manera directa la Fiscalía General de la Nación.

Evaluaremos en concreto si los PSI informan a sus suscriptores sobre esta realidad que impacta en su infraestructura y los datos de las comunicaciones de las personas usuarias de sus servicios, si advierten algo sobre el marco legal en que ésta práctica se orienta, y valoraremos especialmente si hacen explícita su postura o rol ante este tipo de prácticas (como el de pasividad forzada y falta de trazabilidad, por ejemplo).

Para 2021, en este criterio de evaluación destaca el caso de **Movistar** por la claridad con que manifiesta este tipo de realidad. También merece mención los casos de **Claro** y **Tigo** que poco a poco van aumentando el número de PSI que públicamente se manifiestan al respecto.

Movistar ha reportado en su informe de transparencia desde 2017 que, sobre interceptación de las telecomunicaciones "[s]olo se incluyen los requerimiento sobre líneas fijas. Líneas móviles: *No se reportan interceptaciones sobre líneas móviles. La Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptaciones de manera directa sobre las líneas móviles"*[52]. (Subrayado propio)

Se trata de una previsión que es indicativa del acceso directo, que sugiere una distinción entre lo que sucede sobre la interceptación según se trate de líneas móviles o fijas, y que es clara respecto de quién la lleva a cabo.

Tigo por su parte ha decidido manifestar en su informe de "requerimientos de datos personales por terceros y bloqueos de contenido" que "entregamos información personal o damos acceso directo a bases de datos o sistemas que contienen información personal a nuestro cargo a autoridades en ejercicio de sus competencias"(Subrayado propio). Así mismo señala que el Decreto 1704 de 2012 sirve como marco legal de esta práctica.

Es más, según esta misma evaluación efectuada por la Electronic Frontier Foundation sobre Millicom (propietaria de Tigo) en 2019, se evidenció de manera explícita en su informe de transparencia que las autoridades tienen acceso directo a su infraestructura y datos de suscriptores en Colombia:

> **Los procedimientos en Colombia nos obligan a proveer acceso directo a nuestra infraestructura en favor de las autoridades. Auditorías regulares aseguran que nosotros no obtengamos información sobre cuándo una interceptación de este tipo tiene lugar.** *Estamos sujetos a estrictas sanciones, incluyendo multas, si las autoridades averiguan que hemos obtenido información en ese sentido.* **Como resultado de ello, no poseemos información sobre cuán seguido y por qué períodos de tiempo las comunicaciones son interceptadas en uso de nuestra infraestructura en Colombia (Subrayado nuestro)[53].**

Misma situación reportó sobre Honduras, El Salvador y Paraguay, solo que en éste último caso se habilita a los PSI a remitir una queja a la Corte Suprema de ese país en caso de que la orden de acceso directo la encuentren arbitraria o injusta. Algo que no se prevé en el caso Colombiano a favor de los PSI. Este es un tema interesante a resaltar pero no se califica puesto que la información que se evalúa es la del informe local.

52 Ver los informes desde 2016 para Colombia aquí https://www.telefonica.com/es/sostenibilidad-innovacion/privacidad-seguridad/informe-de-transparencia/

53 Traducción propia del documento "Millicom Group Law Enforcement Disclosure Report" de 2019. Ver pg. 10 aquí https://www.millicom.com/media/4222/v4_led-report-2019-002.pdf . Misma información se reportó en 2020 aquí https://www.millicom.com/media/4402/final-millicom-led.pdf , ver pg. 11.

Movistar indicó por primera vez en su informe de transparencia de 2017 que no podía reportar sobre solicitudes de interceptación en sus líneas móviles porque ésto lo hacía directamente la Fiscalía. Como vimos, Millicom, en su informe de 2018 sobre los diferentes países donde opera, también indicó algo similar y **Claro** ese mismo año también señaló en su informe de sostenibilidad una diferencia sobre el régimen jurídico de interceptación de las comunicaciones aplicable entre líneas fijas y líneas móviles. Desde entonces estas empresas han venido informando sobre el tema, si bien hay que resaltar que la información suministrada es especialmente clara en los informes de **Movistar**.

Tanto para el caso de **Claro** como de **Tigo** creemos que vale la pena a futuro intentar una verbalización sobre sus avisos en torno al acceso directo que pueda ser mucho más clara y precisa para los suscriptores de sus servicios. Hacer uso de una distinción como la empleada por **Movistar** o una verbalización como la que citamos de Millicom puede llegar a ser útil para estos efectos.

En definitiva, que en Colombia exista acceso directo de las autoridades a las redes de los PSI sin un marco jurídico claro, sin mediar evaluación de impacto en la privacidad de las personas y sin que haya tenido lugar un análisis profundo sobre su constitucionalidad o compatibilidad con el marco jurídico nacional y compromisos asumidos por el Estado colombiano en materia de derechos humanos, es motivo de preocupación.

La ausencia de controles contrasta con el ejercicio de transparencia que poco a poco han decidido llevar adelante los PSI que son quienes nos ofrecen algún indicio sobre su desarrollo. Más grave aún nos parecen las implicaciones que un aviso como el de Millicom tiene en torno al acceso directo como una condición que puede significar para la empresa un castigo económico, y que merecerá que elevemos las preguntas correspondientes a las autoridades encargadas.

2.4. Solicitudes de datos por parte de entidades públicas, procedimiento de entrega y notificación a las personas sobre dichos eventos

La Ley de Protección de Datos permite la entrega de datos personales a entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial sin autorización de la persona titular de los datos[54]. Las autoridades que reciben la información deben guardarla en reserva, usarla solo para los fines para los cuales la recibieron, deben informar a los titulares del dato sobre el uso que le dan y tomar medidas de seguridad para protegerla[55].

En este eje de evaluación esperamos que las empresas provean información sobre los procedimientos que han diseñado y que siguen internamente a la hora de entregar los datos de las personas que se suscriben a sus servicios a las entidades públicas que los solicitan.

Por *procedimiento interno* nos referimos al proceso de consideración sobre la legalidad y procedencia del pedido antes que al procedimiento desde un punto de vista técnico. Es decir, se trata de establecer si la empresa tiene procedimientos alineados con los derechos humanos.

Por *notificación a las personas usuarias* buscamos identificar si los PSI avisan a sus suscriptores de la entrega de sus datos personales a las autoridades facultadas para requerir acceso a estos. Se trata de promover una buena práctica que aún no tiene recepción legal en Colombia. Con frecuencia se nos indica que dicha notificación no es compatible con la confidencialidad que revisten las investigacio-

54 Ley 1581 de 2012 art. 10 y 13

55 Corte Constitucional. Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

nes preliminares de tipo penal, sin embargo, consideramos que esta afirmación no puede ser llevada a extremos y que -como sucede en otros países de la región como Chile- tal restricción como mínimo debería ser excepcional y limitada a delitos graves, pero entendemos que en este campo existe una discusión que debe darse.

En todo caso, en los años de seguimiento a este informe hemos evidenciado que son diversas las autoridades -no solo las de tipo penal- las que solicitan los datos personales de quienes suscriben los servicios de los PSI y por tanto creemos que la notificación puede tener lugar en el marco de actividades y órdenes de otro tipo, como las que suceden en el ámbito tributario, fiscal o en el marco del logro de políticas sobre beneficios sociales, por citar algunos ejemplos.

En términos generales, creemos que todavía falta avanzar para que se generalice la descripción de los protocolos de atención a las solicitudes de entrega de datos que pueden elevar las autoridades públicas a los PSI.

Durante 2021 los PSI no efectuaron cambios significativos en sus políticas sobre entrega de datos en comparación con la información que ya ofrecían en 2020.

Sobre el procedimiento o protocolo para atender solicitudes de entrega de datos de sus suscriptores con criterios más o menos definidos se destacan **Movistar**, **Tigo**, **DirecTV** y **ETB**.

Por su cuenta, **Claro** solo describe cuáles son las autoridades facultadas para elevar este tipo de solicitudes, sin detallar un procedimiento en este sentido, y Avantel dice tener procedimientos de este tipo pero no los desarrolla ni explica. **EmCali**, **Hughesnet** y **Skynet** no proporcionan ninguna información al respecto.

Queremos resaltar que tanto **Movistar** como **ETB** y **Tigo** tienen los protocolos de trámite para las solicitudes de entrega de datos más fáciles de comprender. Describen en flujos de procesos el paso a paso en que las tramitan, y suelen incluir una fase de validación sobre su procedencia y legalidad.

Sin embargo, ninguna compañía con excepción de **DirecTV** se compromete públicamente a notificar a sus suscriptores de la entrega de sus datos al sector público, compromiso que advierte se hará siempre y cuando ésto sea posible. Habría que advertir que el alcance de este informe no permite verificar su cumplimiento, por tanto sería deseable que **DirecTV** acompañara a esta política con la indicación del número de veces que ha notificado de esto a las personas.

Movistar por su parte, si bien no cuenta con procesos de notificación a sus suscriptores, despliega mecanismos de protección a los derechos de sus usuarios. Señala que en la validación de la procedencia de las solicitudes de acceso a sus datos personales, aplica los principios de: confidencialidad en su trámite, exhaustividad y fundamentación de la orden, proporcionalidad y neutralidad política de la misma, respuesta diligente en su trámite y seguridad en la entrega de los datos.

De contexto e interés

Y si bien el proceso de notificación a las personas suscriptoras de este tipo de eventos es todavía excepcional, es una buena práctica que merece un análisis cercano para evaluar su conveniencia, especialmente a partir de las solicitudes de entrega de datos que fueron elevados en repetidas ocasiones a los PSI a raíz de la pandemia y que fueron efectuados en casos como los de constitución de la base maestra de datos para identificar y notificar a las personas beneficiarias del Programa Ingreso Solidario (PIS).

Según noticia reciente, supimos por la publicación del medio La Silla Vacía que el abonado celular de

las personas beneficiarias de dicho programa y que fue entregado por los PSI al Departamento Nacional de Planeación[56], fue accedido de manera irregular por terceros no autorizados con el fin de publicitar campañas políticas en el marco de la contienda electoral que tendrá lugar en marzo de 2022[57].

La notificación previa, en este tipo de casos, podría ayudar a informar a las personas afectadas permitiéndoles una mayor trazabilidad de su información en la pregunta sobre *dónde están sus datos.* Si bien no es deber de los PSI evitar la ocurrencia de situaciones como la documentada por La Silla Vacía, procesos como la notificación sobre la entrega de sus datos al Estado podría llegar a habilitar a las personas para reclamar de manera informada ante la autoridad de protección de datos y exigir la rendición de cuentas sobre lo sucedido.

Así mismo, genera particular inquietud la ausencia de información sobre la atención a solicitudes de acceso a datos personales elevados por autoridades públicas ante empresas como **Emcali**, de la que es propietaria el Estado. En este sentido, creemos que los PSI en donde el Estado es accionista o propietario deben publicar y adoptar políticas de transparencia en la entrega de datos de sus suscriptores con un estándar más elevado, dada su naturaleza.

También echamos en falta información detallada en el caso de **ETB** que informe cómo se da curso a las solicitudes de entrega de datos cuando las solicitan entidades en donde la empresa tiene participación como accionista. Es el caso de la Agencia de Analítica de Datos de Bogotá, AGATA[58], y que fue constituida en 2020 por ETB, el Grupo de Energía de Bogotá, la Empresa de Acueducto y Alcantarillado de Bogotá, la Unidad Administrativa Especial de Catastro Distrital y la Secretaría Distrital de Planeación. Según el portal web de dicha Agencia, los miembros de la alianza proveen las fuentes de información (¿incluirá los datos de las personas suscriptoras de dicho PSI y en caso afirmativo, se informará a su titular?) para proveer información analítica que apoye la toma de decisiones.

En una petición de acceso a la información que dirigimos en 2021 a AGATA[59], y en la que preguntamos sobre el origen de las fuentes de información y los usos a los que estarían destinados, supimos que dicha agencia podrá acceder a "las bases de datos que se encuentren en poder de cualquier entidad u organismo del Distrito Capital de Bogotá, del sector central, del sector descentralizado o el de las localidades" a fin de cumplir con su objeto social que es aportar "a la visión de *Smart City* y de transparencia de la Bogotá del Siglo XXI"[60] y cuyos servicios "podrá comercializar" al sector privado.

En futuras ediciones de nuestro informe seguiremos de cerca este tipo de iniciativas que podrán llegar a justificar una evaluación mucho más exigente en materia de transparencia sobre la compartición de datos personales que efectúan empresas en donde el Estado es accionista o propietario.

56 Resolución 1093 de 2020 "el Departamento Nacional de Planeación -DNP en coordinación con los operadores de telefoná celular adelantará la ubicación de beneficiarios no bancarizados e implementará una estrategia de bancarización digital a través de números de telefonía celular", art. 2, lit. c.

57 Sugerimos consultar el artículo de Jineth Prieto publicado en La Silla Vacía titulado "Uribismo hace campaña con bases de datos de Ingreso Solidario en Santander" https://www.lasillavacia.com/historias/silla-nacional/uribismo-hace-campana-con-bases-de-datos-de-ingreso-solidario-en-santander/?s=09

58 Constituida a través del Decreto Distrital 272 de 2020.

59 Petición que fue identificada bajo el radicado 827722021, respondida el 20 de abril por la Agencia de Analítica de Datos.

60 Ver justificación del Decreto 272 de 2020.

3. Eje sobre libertad de expresión

3.1. Obligación legal de bloqueo y el procedimiento de bloqueo

El bloqueo de sitios web o URL son medidas de excepción que deben estar reguladas en la ley. Ordenes de este tipo solo proceden como medida de protección de un derecho humano u otro interés legítimo[61].

En Colombia la protección de esos intereses legítimos ha dado paso a cuatro subtipos de bloqueo legal en particular, y que son: el bloqueo de sitios web en que circulan contenidos sobre el abuso sexual infantil en línea[62], el bloqueo para combatir la ilegalidad en los juegos de suerte y azar[63], las órdenes de bloqueo de tipo judicial y administrativo, y las órdenes de bloqueo que tienen lugar durante los estados de emergencia y excepción[64].

Existen también eventos en que los PSI advierten en los términos y condiciones de prestación de sus servicios que podrían llegar a bloquear sitios web o URL por razones de tipo contractual. En este tipo de escenarios, pedimos a los PSI implementar procedimientos de reclamo en favor de las personas usuarias.

En nuestra evaluación nos interesa verificar, en concreto, que los PSI reconozcan que llevan a cabo este tipo de medidas y que cuentan con un procedimiento para tramitarlas. Explicar el procedimiento es un acto de transparencia en la manera en cómo se ejecuta el bloqueo, independientemente de si su origen es de tipo legal o contractual.

En la explicación de dicho procedimiento también verificamos si se prevé un paso de notificación a las personas usuarias de sus servicios sobre el tipo de bloqueo efectuado, el marco legal y la razón en que éste se motiva.

En nuestra revisión encontramos que **Claro**, **Movistar**, **Tigo**, **ETB** y **Avantel** informan sobre la ejecución de órdenes de bloqueo de sitios web o URL.

Movistar informa a plenitud sobre todos los tipos de bloqueo de sitios web o URL que puede efectuar. Cuenta con un procedimiento detallado para tramitar solicitudes de bloqueos de sitio web y URL. Y también notifica a sus suscriptores del tipo de bloqueo que efectúa en cada caso, anunciado el soporte legal en que se motiva cada uno.

Claro es el único PSI que informa expresamente en su informe de transparencia que no efectúa bloqueos de sitios web o URL de naturaleza contractual. Sin embargo, pese a contar con un procedimiento de bloqueo, no anuncia a las personas usuarias de sus servicios cuándo un sitio web o URL han sido bloqueados, o la razón de ello.

Tigo cuenta con un procedimiento detallado de bloqueo, así como informa que notifica a las personas usuarias de sus servicios cuando un bloqueo de sitio web o URL ha tenido lugar, así como el motivo en que dicha medida se justifica.

61 Esto es así según el estándar interamericano fijado por la Relatoría para la Libertad de Expresión de la Organización de Estados Americanos. Al respecto se puede ver el informe "Estándares para una Internet Libre, Abierta e Incluyente", que se puede consultar aquí http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

62 Según lo contenido en el art 7 y art 8 de la Ley 679 de 2001; art. 5 y art. 6 del Decreto 1524 de 2002

63 Según lo ordena el art. 38 de la Ley 643 de 2001.

64 Según el art. 8 de la Ley 1341 de 2009.

Avantel avisa que lleva a cabo bloqueos de sitio web o URL de naturaleza contractual sin proveer información sobre si cuenta o no con procedimientos de reclamo para que las personas suscriptoras que estimen que se trató de un procedimiento arbitrario puedan solicitar una revisión de dicha medida. Esta compañía cuenta con un procedimiento para dar trámite a este tipo de eventos pero no informa en qué consiste.

Emcali y **Hughesnet** informan que bloquean sitios web o URL solo en el caso de circulación de contenido de abuso sexual infantil. **Skynet** no provee información sobre ninguno de estos criterios.

De contexto e interés

El 15 de septiembre de 2020 se documentó por primera vez la imposición de una medida cautelar de bloqueo de sitio web o URL en materia de derecho de autor[65].

La Dirección Nacional de Derechos de Autor ordenó a **Claro**, **ETB**, **Tigo**, **Movistar** "y demás proveedores de acceso a Internet" que bloquearan de manera temporal la retransmisión hecha por una persona en internet (Facebook, concretamente) sobre una señal con contenido deportivo respecto de la cual su titular (reservado en el expediente) no había concedido permisos a terceros para retransmitirla en la web.

Es importante señalar que el bloqueo de URL o sitios web por la retransmisión ilegal de contenidos en internet no se encuentra plenamente regulado en Colombia. El marco jurídico aplicable es la Ley en derecho de autor que data de 1982 y que no responde a las dinámicas de Internet.

Dicha ley junto al Código General del Proceso consagran la imposición de medidas cautelares que habilitan al titular del derecho de autor a interrumpir la continuación de la vulneración de su derecho, pero ni la Ley ni el Código ofrecen elementos de valoración que permitan articular el impacto de la medida con la arquitectura de internet y el respeto por sus principios fundantes.

En torno a su motivación, la medida es más bien escueta. Afirma que "con la finalidad de evitar las consecuencias derivadas de la posible infracción, prevenir los posibles daños con el despliegue de conductas que quieren evitarse con la medida cautelar propuesta y asegurar la efectividad de la pretensión, considera este Despacho que se encuentra justificada en derecho"[66]. A la fecha desconocemos si esta medida cautelar sigue en pie.

En el marco de las órdenes de bloqueo "de origen legal y administrativo" hemos visto también un crecimiento en el número de órdenes de bloqueo temporal de sitios web dirigidas a la protección de datos[67] de las personas, y que son emitidas por la SIC y su Delegatura de Protección de Datos.

La orden de bloqueo temporal de datos se encuentra prevista en el artículo 21 (lit. c) de la Ley 1581 de

65 Accedimos a la medida cautelar a través de una solicitud de acceso a la información. La respuesta se identificó con el radicado 1-2-21-25964. La medida cautelar se identifica bajo el radicado 1-2020-86220, suscrita por la Subdirección de Asuntos Jurisdiccionales de la Dirección Nacional de derecho de autor, Auto 04 del 15 de septiembre de 2020.

66 La medida cautelar se identifica bajo el radicado 1-2020-86220, suscrita por la Subdirección de Asuntos Jurisdiccionales de la Dirección Nacional de derecho de autor, Auto 04 del 15 de septiembre de 2020, ver pg. 9

67 Aunque esto seguramente lo analizaremos en nuestro informe en que evaluemos lo sucedido en 2021, es importante documentar el incremento que estos bloqueos están teniendo. Así, mientras en 2018 se reportó un solo caso (bloqueo del sitio web de pig.gi según la Resolución 20568 de 2018 y 21215 de 2018), en 2021 se documentaron al menos ocho casos (bloqueo del sitio web de Ocupar Temporales según la Resolución 64453 de 2021; bloqueo del sitio web de Colombia Reports según la Resolución 46344 de 2021; el bloqueo de URL en Twitter y Telegram según la Resolución 37376 de 2021; el bloqueo de sitio web de Ghostbin y Archive.org según la Resolución 37070 de 2021; bloqueo del sitio web de WOM Colombia según la Resolución 19163 de 2021; bloqueo del sitio web de Avantel S.A.S según la Resolución 12734 de 2021; bloqueo de sitio web de la Fuerza Aérea Colombia según la Resolución 970 de 2021; bloqueo del sitio web de la Fundación Talentum según Resolución 842 de 2021).

2012 que faculta a la SIC a ordenar de manera preventiva el bloqueo de sitios web en los eventos en que se difunden datos personales sin la autorización de su titular.

Para la procedencia de esta medida, la persona afectada debe (i) solicitar a la SIC expresamente su imposición, (ii) debe tratarse de la difusión no autorizada de datos que consten en una base de datos identificable y amparada bajo el marco de aplicación de la ley de protección de datos, y (iii) se deben aportar pruebas que permitan constatar a la autoridad que la difusión no consentida de los datos personales constituyen un riesgo cierto para el ejercicio de sus derechos.

Cuando la protección de datos se encuentra en conflicto con otros derechos como el de la libertad de expresión, la autoridad de protección de datos se debe abstener de imponer este tipo de medidas en tanto que no es competente para valorar conflictos entre derechos fundamentales y que requieren la valoración de un juez de la república.

Más recientemente hemos visto cómo ha habido casos en donde se ha discutido la imposición de medidas de bloqueo temporal de datos y se ha decidido sobre su procedencia, incluso respecto de casos en donde la libertad de expresión se encuentra en juego. En futuras ediciones valoraremos que los PSI puedan a futuro desagregar el tipo de bloqueo según la autoridad administrativa que la emite (como en el caso de la DNDA o la SIC) y que dichas órdenes se vean reflejadas con mayor detalle en sus informes de transparencia anual.

4. Eje sobre seguridad digital

En este eje, se evalúa si las compañías informan las fugas de datos personales y acciones de mitigación en caso de que se presenten, si tienen protocolos de notificación a las autoridades cuando suceden fallas de seguridad que comprometen los datos personales de las personas usuarias de los servicios, así como si las notifican sobre estos sucesos luego de que hayan desplegado las debidas medidas de mitigación. También tomamos nota de los portales web de cada operador y que en efecto usen un protocolo de seguridad *https*.

Mientras que todos los operadores han incluido el certificado de seguridad en sus portales, solo tres operadores cuentan con políticas públicas para el manejo de fugas de datos. Esta información no ha variado en comparación a los hallazgos de 2020.

Movistar, **Tigo** y **Avantel** son las únicas que cuentan con un protocolo y documentación para realizar acciones de mitigación y bloqueos. Skynet advierte en general qué medidas de seguridad despliega pero no cuáles son las de contingencia que aplicaría para posibles brechas de seguridad.

Movistar advierte en su Centro de Privacidad que notificará a las autoridades ante eventos de fuga, que notificará a las personas suscriptoras de sus servicios y que hará públicas las acciones empleadas para la mitigación.

Tigo expresa en su documento titulado "Requerimiento de datos personales por terceros y bloqueos de contenido" que ante incidentes de seguridad cumplirá con la obligación legal de reportarlo ante la Superintendencia de Industria y Comercio, así como notificará a sus suscriptores de un "mecanismo eficaz (...) y las medidas realizadas por la compañía para disminuir el riesgo".

Avantel prevé en su política de tratamiento de datos que notificará a la autoridad cuando "se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares", así mismo asume como deber "informar y apoyar el responsable en la gestión de incidentes de

seguridad de la información que comprometan información personal de los cuales tenga conocimiento o que sean informados al responsable". Si bien no expresa que notificará a las personas suscriptoras de sus servicios sobre eventos de este tipo, sí señala que emprenderá las acciones de mitigación que sean pertinentes en cada caso.

Finalmente, pudimos validar que todos los PSI evaluados han implementado el protocolo https en sus sitios web.

Recomendaciones

La transparencia en la información es un instrumento clave en la exigencia y la realización de otros derechos. Los proveedores de acceso y servicios de internet en Colombia han avanzado con políticas en la concreción de una mayor transparencia sobre sus actividades comerciales que impactan en la libertad de expresión, privacidad y seguridad digital de las personas usuarias de sus servicios. Tal y como hemos documentado a lo largo de estos seis años de *¿Dónde están mis datos?*, se trata de pasos significativos en la consolidación de sus compromisos con los derechos humanos.

Creemos que en esta etapa en que nos encontramos, el camino que hay que recorrer transita por afinar las políticas existentes en un mayor detalle y precisión: más y mejor información redunda en beneficio de todas las personas que orientan mejor sus procesos de toma de decisión sobre qué servicio adquirir con qué ISP, también ofrecen más luz sobre las prácticas opacas de las autoridades.

Nuestras recomendaciones en el *eje de compromisos políticos* apuntan en concreto a:

- Incentivar a las compañías que aún no adoptan compromisos en materia de género y accesibilidad a que emprendan esfuerzos en este sentido. No solo porque se precisa de una mayor representación del resto de la sociedad en un sector crítico como el de las tecnologías, sino porque mayor diversidad significa a su vez un paso afirmativo hacia la igualdad en escenarios donde todas las voces merecen participar, tomar la palabra y ser visibilizadas.
- En materia de transparencia creemos que los PSI que aun no publican información sobre solicitudes de datos de sus suscriptores, bloqueos de URL e interceptación de las comunicaciones deben hacerlo, no solo por los mandatos legales vigentes que los obligan a ello, sino porque facilitan a su vez el ejercicio de un mayor escrutinio sobre las actividades y obligaciones a cargo del Estado en cada una y respecto de la que éste no provee información activamente.
- En materia de neutralidad de la Red instamos a los PSI a ir más allá de la publicación de sus prácticas de gestión del tráfico, haciendo público y expreso su compromiso por proteger el principio de neutralidad de la Red.

Nuestras recomendaciones en el *eje de intimidad* enfatizan en:

- Ver las buenas prácticas que otros PSI han adoptado para garantizar la protección de los datos de las personas usuarias de sus redes a través de la implementación, por ejemplo, de análisis de impacto en privacidad, o reservando para sí la realización de auditorías en dicha materia respecto de socios comerciales con los que se suscriben acuerdos.
- Se precisa implementar procesos de notificación de las personas suscriptoras de sus servicios para

que estén enteradas sobre los eventos de compartición de sus datos personales con el Estado. El caso del Programa Ingreso Solidario torna urgente este tipo de acciones que habilitan a las personas al reclamo y mejor ejercicio de sus derechos ante las autoridades públicas.

- Sobre la retención de los datos de las personas usuarias de los servicios de los PSI se precisa, en general, de mayor información sobre lo que significa en la práctica almacenar y conservar esta información, incluso por un período de tiempo mucho mayor al que prevé la ley colombiana. Se requiere de una mayor compatibilidad entre las prácticas y las normas que regulan esta materia.
- Sobre el acceso directo invitamos con vehemencia a los PSI a que informen sobre si experimentan una situación como la descrita por Claro, Movistar y Tigo en sus reportes de transparencia anual. Esta información es una vía que habilitará el escrutinio y la rendición de cuentas a cargo del Estado, pero para ello es importante que las compañías decidan informar sobre si el acceso directo es una realidad que pesa sobre su infraestructura y datos de las personas que usan sus servicios. Al tiempo, es importante que hagan saber a estas personas cuáles son las limitaciones que les impiden efectuar un rol de protección o resguardo de la privacidad de éstos últimos.

Nuestras recomendaciones en el eje de libertad de expresión:

- Es preciso que se pueda informar con mayor detalle sobre las estadísticas de bloqueo de sitios web y URL en cada uno de los eventos que se encuentran regulados o que tienen lugar en Colombia pese a la ausencia de regulación específica para casos como el de los bloqueos por derecho de autor.
- En tanto que en la edición que viene documentaremos la información que proveen sobre los bloqueos de URL y sitios web que tuvieron lugar durante el paro nacional en 2021, creemos que es importante aumentar el detalle del procedimiento de atención a estas órdenes, así como las instancias de evaluación y rechazo que pueden insistir en su inaplicación por el impacto que tienen en el ejercicio del derecho a la libertad de expresión de sus suscriptores.

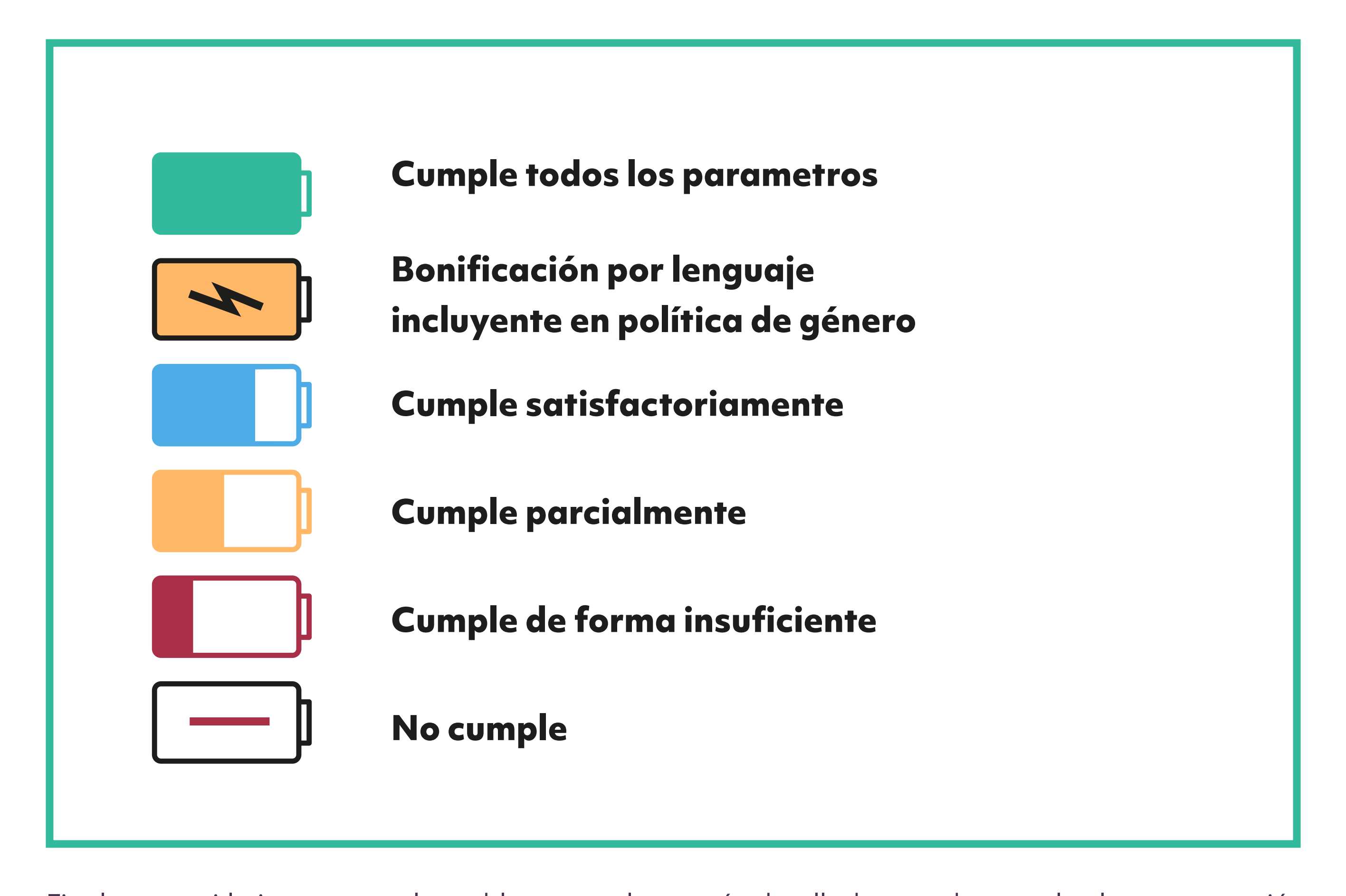
Finalmente, nuestras recomendaciones en el *eje de seguridad digital* enfatizan en:

- Comprometerse con notificar en tiempo y forma a las personas usuarias afectadas en brechas de seguridad digital que expongan su información personal y sensible. Este tipo de procedimientos cuando son desplegados de manera activa pueden incluso llegar a fortalecer la imagen y credibilidad de una compañía que decide ser transparente y honesta con sus suscriptores.
- Se precisa de compromisos públicos sobre el mismo procedimiento de notificación pero respecto de la autoridad de protección de datos. Pese a que pueda constituir un evento que llame la atención del regulador sobre la compañía, hacerlo de manera proactiva es también cumplir en tiempo con un deber legal consagrado en la Ley de Protección de Datos.

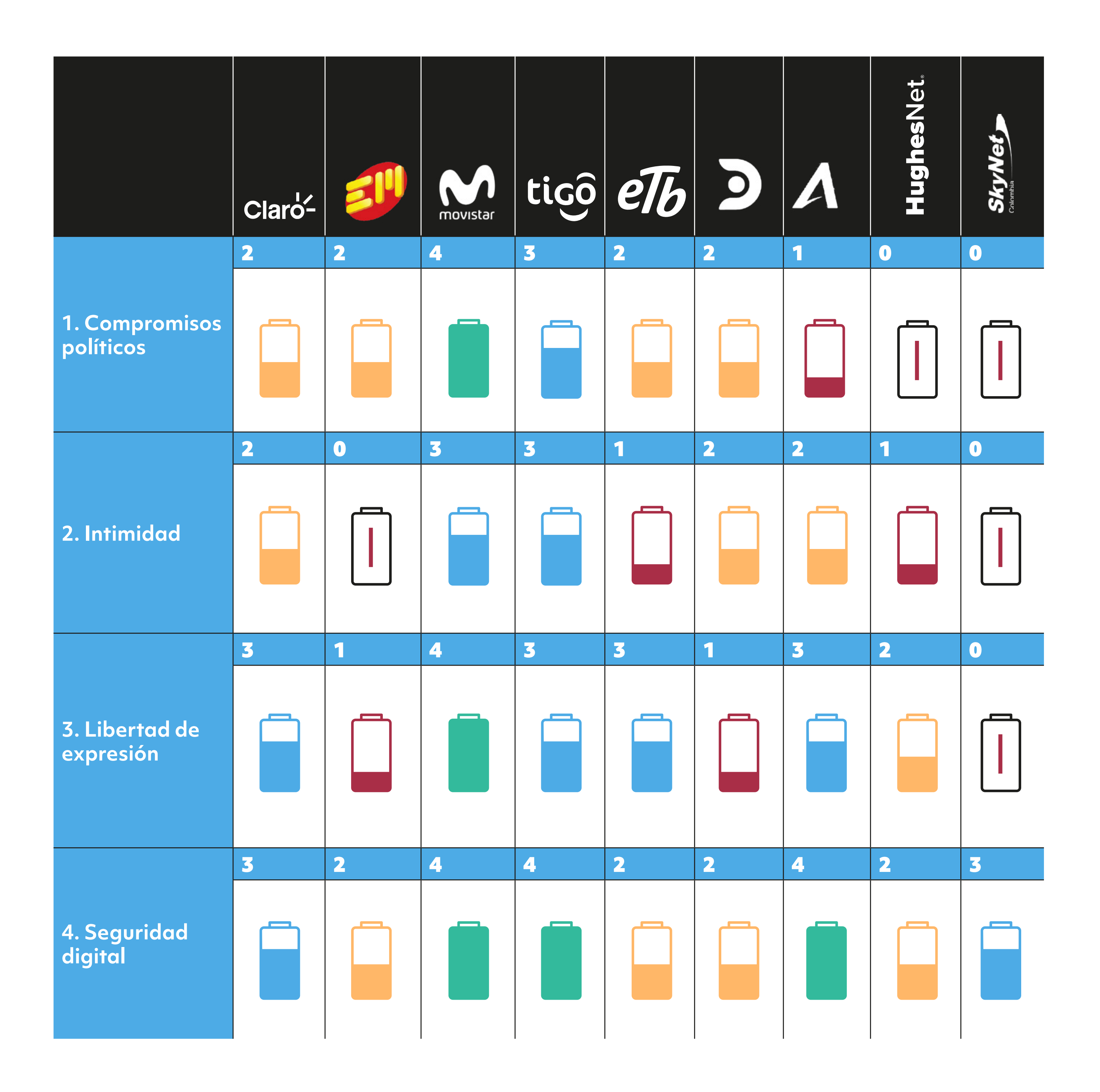
En general, queremos instar a los proveedores de internet satelital a imitar los progresos de esos otros de mayor tamaño y cobertura. Su rol como proveedores del acceso a internet en la ruralidad no es de menor impacto o de reducida importancia: ustedes también son actores que precisan estar a tono con los compromisos y buenas prácticas en derechos humanos vigentes en el sector de las telecomunicaciones.

Las gráficas ¿Dónde están mis datos?

Los datos de la evaluación de cada empresa se reflejan en las siguientes gráficas:



Finalmente, si le interesa ver las tablas con valores más detallados puede consultarlas en su versión digital en https://web.karisma.org.co/donde-estan-mis-datos-2021/



	Claro		movistar	tigo	eTb			HughesNet	SkyNet Colombia
1. Compromisos políticos	2	2	4	3	2	2	1	0	0
2. Intimidad	2	0	3	3	1	2	2	1	0
3. Libertad de expresión	3	1	4	3	3	1	3	2	0
4. Seguridad digital	3	2	4	4	2	2	4	2	3

	Claro	EM	movistar	tigo	eTb	D	A	HughesNet	SkyNet Colombia
Compromisos politicos	2	2	4	3	2	2	1	0	0
1.1. Política de género									
1.2. Política de accesibilidad									
1.3. Informes de transparencia									
Intimidad	2	0	3	3	1	2	2	1	0
2.1. Políticas de protección de datos									
2.2. Informa la obligación legal de retención de datos									
2.3 Acceso directo									
2.4. Informa las razones para responder a solicitudes de información del sector público									
2.5. Procedimiento de entrega de datos al sector público									
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas									
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales									
Libertad de expresión	3	1	4	3	3	1	3	2	0
3.1. Informa sobre la obligación legal de bloqueo									
3.2 Procedimientos de bloqueo (incluye obligación contractual)									
3.3. Guía sobre comportamientos no permitidos									
Seguridad Digital	3	2	4	4	2	2	4	2	3
4.1. Informa de fuga de datos personales y acciones de mitigación									
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web									

Claro	Suma por criterio	Promedio por eje 2020	Promedio por eje 2021
1. Compromisos políticos		2	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	2
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		3	3
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

movistar	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		4	4
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		3	3
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		4	4
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		4	4
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

eTb	Suma por criterio	Promedio por eje 2020	Promedio por eje 2021
1. Compromisos políticos		1	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		1	1
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

DIRECTV	Suma por criterio	Promedio por eje 2020	Promedio por eje 2021
1. Compromisos políticos		**0**	**2**
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		**2**	**2**
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		**3**	**1**
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		**2**	**2**
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

tigo	Suma por criterio	Promedio por eje 2020	Promedio por eje 2021
1. Compromisos políticos		1	3
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	3
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		4	4
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

EMCALI VALORAMOS LO ESENCIAL	Suma por criterio	Promedio por eje	
		2020	2021
1. Compromisos políticos		2	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		0	0
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		0	1
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

Avantel LTE PRO	Suma por criterio	Promedio por eje 2020	Promedio por eje 2021
1. Compromisos políticos		0	1
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	2
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		4	4
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

HughesNet	Suma por criterio	Promedio por eje 2020*	Promedio por eje 2021
1. Compromisos políticos			0
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad			1
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión			2
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital			2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

*La compañía se incluyó en este informe desde el año 2021, por tanto, no se reportan datos para el 2020.

SkyNet Colombia	Suma por criterio	Promedio por eje	
		2020*	2021
1. Compromisos políticos			0
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad			0
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Acceso directo			
2.4. Informa las razones para responder a solicitudes de información del sector público			
2.5. Procedimiento de entrega de datos al sector público			
2.6. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.7 Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión			0
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital			3
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

*La compañía se incluyó en este informe desde el año 2021, por tanto, no se reportan datos para el 2020.



Informe

¿DÓNDE ESTÁN MIS DATOS?

2021: una mirada retrospectiva a la pandemia

El informe ¿Dónde están mis datos? 2021 es la sexta publicación que realiza la Fundación Karisma de esta serie.

Esta investigación busca que las empresas proveedoras de internet ofrezcan más información a sus usuarios para que mejoren su capacidad de hacer efectivos sus derechos humanos.

Para conocer y descargar el texto completo de este año visita: https://web.karisma.org.co/donde-estan-mis-datos-2021/

Puedes conocer los informes anteriores en https://karisma.org.co/DEMD/

Un informe de:

Fundación Karisma

Con el apoyo de:



